'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.		
20	The system of claim 12, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
21	The system of claim 20, wherein an enterprise monitor associated with a	See '203 claim 10	See '203 claim 10

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.		

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service	See '203 claim 1	See '203 claim 1

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	protocols};		
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
5	The method of claim 1, wherein the enterprise network	See '203 claim 5	See '203 claim 5

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	is a TCP/IP network.		
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"*NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: … The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966] "Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			"The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] See Figure 12 in my expert report. --- "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111] "Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered: 1.3.6.1.4.1.42 The "Flintstones, Inc " enterprise might then register their "Fred Router" under the name of: 1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017] "See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013] "sysServices OBJECT-TYPE . . . ' . . . layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays)

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			For systems including OSI protocols, layers 5 and 6 may also be counted.'" (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156] "ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1). -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165] "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.		**103:** *See* Feather, Frank Edward, Ph.D., "Fault Detection in an Ethernet network via anomaly detectors", Carnegie Mellon University, Order number 9224199, 1992 [SYM_P_0501779- SYM_P_0502036].
8	The method of claim 1,	See '203 claim 7	See '203 claim 8

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.		
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain	See '203 claim 10	See '203 claim 10

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	monitors within the enterprise network.		
13	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '615 claim 1	See '615 claim 1
	said network monitors	See '615 claim 1	See '615 claim 1

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	generating reports of said suspicious activity; and		
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of	See '203 claim 4	See '203 claim 4

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	third-party tools.		
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '615 claim 6	See '615 claim 6
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
21	The system of claim 13,	See '203 claim 9	See '203 claim 9

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	*"NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: ... The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]

NetStalker and HP OpenView

"615" Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
		"Initial PC Filter Configuration *NetStalker* has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and *NetStalker.* The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing *NetStalker."* p. 1-4. [SYM_P_0079562] *"Securing the Connection* Since the *Netstalker* server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the *NetStalker* server platform. The most efficient means of protecting this connection between the NSC router client and the *NetStalker* is to use separate BorderGuard routers between the *NetStalker* platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the *NetStalker* platform. Since all IP traffic between the *NetStalker* platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties. Alternatively, the *NetStalker* platform can be located on an individual network segment that is directly connected to a dedicated port on the	"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958] "The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] See Figure 12 in my expert report. ----------

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
		router it is monitoring." p. 1-4. [SYM_P_0079562] "Before *Netstalker* can protect your network, you must configure the program for your site by setting up the routers to be monitored. This chapter describes how to add and edit client routers listed in the *NetStalker* window. It also describes how to verify the client information . . ." pp. 3-1-3-6. [SYM_P_0079577-SYM_P_0079582]	"Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111] "Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered: 1.3.6.1.4.1.42

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of: 1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017] "See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013] "sysServices OBJECT-TYPE . . . ' . . . layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) For systems including OSI protocols, layers 5 and 6 may also be counted.'" (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156] "ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165] "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
35	The method of claim 34, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
36	The method of claim 34,	See '203 claim 3	See '203 claim 3

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	wherein said integrating further comprises invoking countermeasures to a suspected attack.		
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
39	The method of claim 34, wherein said deploying the network monitors includes placing a plurality of service	See '203 claim 7	See '203 claim 7

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	monitors among multiple domains of the enterprise network.		
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
41	The method of claim 34, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
42	The method of claim 41, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a router;	"*NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560] "***Initial PC Filter Configuration*** *NetStalker* has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and *NetStalker*. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing *NetStalker*." p. 1-4. [SYM_P_0079562] "***Securing the Connection*** Since the *Netstalker* server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the *NetStalker* server platform.	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: ... The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966] "Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics